A Blockchain Based Cloud Integrated IoT Architecture Using a Hybrid Design

Ch Rupa[1(✉)], Gautam Srivastava[2], Thippa Reddy Gadekallu[3], Praveen Kumar Reddy Maddikunta[3], and Sweta Bhattacharya[3]

[1] Department of Computer Science, VR Siddhartha Engineering College, Vijayawada 520007, India
rupamtech@gmail.com

[2] Department of Mathematics and Computer Science, Brandon University, Brandon, MB R7A 6A9, Canada
srivastavag@brandonu.ca

[3] School of Information Technology and Engineering, VIT - Vellore, Tamilnadu, India
{thippareddy,praveenkumarreddy,sweta.b}@vit.ac.in

Abstract. The Internet of Things (IoT) and its applications are gaining popularity in recent years due to features like ease of use and increased availability of the Internet. We can enhance the efficiency of IoT based systems by adding other advanced technologies like cloud infrastructure and blockchain technology. Through these enhancements IoT applications can be accessed at any time from any place. However, a database is required for storing the information of the application. Cloud infrastructure is an ideal solution for storing IoT based applications as it provides remote services such as storage, computation, and analysis. The major drawback of these applications are their inability to provide security and privacy for data. Blockchain technology helps in overcoming these drawbacks with features like immutability, transparency, and distributed structure. In this paper, a blockchain based cloud integrated IoT application is proposed that can assist to identify intruders through virtual monitoring. The main advantage of this application is that it can operate in areas where manual monitoring is challenging and data is stored in a blockchain-based tamper-free environment.

Keywords: Internet of Things · Cloud infrastructure · Centralized system · Blockchain technology · Distributed system

1 Introduction

Globally, attention to the Internet of Things (IoT) as well as Unmanned Aerial Vehicles (UAV) is growing tremendously. There are numerous applications based on IoT and UAV technologies such as in Healthcare, Vehicular, Surveillance, and in the Government sector [27–29]. According to the Information Handling Services (IHS) Markit report, in 2018, about 20 billion devices were connected

H. Gao et al. (Eds.): CollaborateCom 2020, LNICST 350, pp. 550–559, 2021.
https://doi.org/10.1007/978-3-030-67540-0_36

to the Internet, and about 1.2 billion IoT devices were installed. The numbers might be extended up to 125 billion by 2030 [30]. These analytics clearly show that IoT/UAV devices can be used to improve the services for society. The main features of the IoT/UAV technology are "CCCC" (Connections, Collection, Computation, Creation) which are interconnected to each other [22,33].

Global data transmission rates are expected to rise by about 20%-50% per year, on average [25]. Data protection from unauthorized access is an important task while using IoT/UAV devices. Previously the databases that are based on CRUD (Create, Read, Update, and Delete) operational model used to store the data [47]. Later cloud computing has gained popularity as it overcomes the disadvantages of databases. Cloud data can be accessed from any place and at any time [24,38,39]. Currently, one emerging technology, Blockchain, is impacting all database based applications because of its key features like immutability, transparency, distributed computing, and security [12,20,43,44]. Cyber attacks on the cloud is also on the rise [10,18].

Many sectors such as smart grid, Supply Chain Management, finance, cryptocurrencies, insurance, smart cities, and many others [15,32] are using blockchain technology to enhance credibility. The main reason behind the success of blockchain technology is consensus algorithms like Proof-of-Work (PoW), Proof-of-Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), etc. Consensus algorithms play a major role in securing the sensitive details from the hackers; if any detail has to be modified in the blockchain, it has to be agreed upon by a majority of nodes through consensus. Consensus algorithms are the main reason behind the trustworthiness of nodes in blockchain networks. If any new node has to be added into the network, a majority of the nodes have to agree that the new node is trustworthy through consensus algorithms [26,49]. Another important concept in blockchain technology is smart contracts. Smart contracts are the codes which will be automatically executed in the blockchain network whenever a transaction occurs, to ensure that the transactions adhere to preconditions [48]. Blockchain technology [6,13] helps in reducing attacks on surveillance data collected from IoT/UAV devices. The information maintained by using blockchain technology along with cloud infrastructure can improve the security and privacy of data. Generally, any application communicates with the cloud to store collected data from the application gateway. Later, the data is processed and analyzed in real-time using batch analytics, visualization, and machine learning [36]. Various Cloud platforms like Open stalk, GCP (Google cloud platform), Microsoft Azure are available to design and develop such systems [14].

In the proposed system, we used the Open Stalk cloud platform and Ethereum in Ganache with a meta mask wallet for blockchain technology [21,35,37]. In this paper, we propose a methodology by considering an IoT based application such as a virtual circuit based vehicle monitoring system (VVMS). The collected data from the VVMS is stored, processed, and analyzed on the cloud. Instructions are received by the vehicle through an operator virtually, along with the VVMS responses for instructions are stored on the blockchain

and on the cloud. Such an infrastructure can protect information from various cyber attacks like ransomware, known ciphertext attach, injection attacks [2,8], and other malware attacks [1,11].

The rest of the paper is organized as follows. Section 2 discusses about the literature survey related to the concepts and required architectures of the proposed system. Proposed system architecture and implementation results are discussed in Sect. 3. Section 4 gives an in-depth conclusion and future scope of this work.

2 Related Works

Anthi *et al.* [4] proposed a three-layer intrusion detection system [7,40] to defend IoT devices. The main functions of this system are the classification of device behavior and identification of suspected packets (malicious packets) and classify the attacks. The main drawback of this approach is that anyone can modify or update the data over the network like a man in the middle attack. This system cannot be operated at any time from any place as it is designed as a standalone system.

Ullah *et al.* [19] developed an IoT based system to detect lightweight attacks in terms of the Intrusion detection system (IDS). Here the authors used support vector machine-based supervised machine learning for identifying the injection attacks over the IoT network. Arshad *et al.* [5] discussed intrusion detection system (IDS) using IoT and mentioned the open challenges to achieve Intruder detections over IoT Infrastructure. In this paper, the authors proposed an IDS system by following the signature, specification, Anomaly and hybrid-based approach. The main limitation of this work is its lack of privacy.

Sabir *et al.* [42] proposed a driver-friendly interface system that can monitor the speed breakers and potholes by monitoring the roads. Crowdsourcing approach was used to design and develop the system. The main limitations of this system are the lack of privacy and preservation of the data which are captured by the proposed interface. Also there is no information about the data storage locations, access and computation specifications on the data.

Hu *et al.* [16] designed a smart vehicle system using IoT with embedded control. This system can automatically chase the light source and monitors the vehicle moving directions and its path. In the same way, Metlo *et al.* [31] proposed a system to track vehicles using GPS. In this work, authors have considered the GPS data as an input to the tracing algorithm to detect specific vehicles based on crowdsourced data. The main limitations of these works are lack of security to the information. Also there is no transparency and reliability in the proposed system.

Ali *et al.* [3] discussed the role of blockchain in the IoT. Here authors have explained clearly how blockchain-based systems can achieve the characteristics like security, immutability, and decentralization. This paper explained how the challenges faced by IoT systems that are based on centralized architecture can be solved by using blockchain (Table 1).

Table 1. Comparative analysis of existing approaches for IoT

Approaches	Characteristics					
	Is blockchain based?	Transparency	Immutable	Architecture	Visibility	Application
[34]	No	No	No	Centralized	Host	IDS
[23]	No	No	No	Centralized	Network	IDS
[17]	No	No	No	Centralized	Host	IDS
[9]	No	Yes	No	Distributed	Network	IDS
[41]	No	No	No	Centralized	Host	IDS
Proposed method	Yes	Yes	Yes	Distributed	Host	IDS through VMSS

3 Proposed Methodology

A proposed blockchain-based cloud-integrated IoT based application enhances the privacy of data while maintaining efficiency in both computation and energy use. The proposed system detects intruders by virtual monitoring and operating the vehicle. The design and development of the proposed IoT system uses Node MCU, Arduino, Motor drivers, camera, and mobile devices as connected devices (IoT). A gateway is required to transfer data from IoT connected devices to the cloud for maintaining the communication data. Therefore, Blynk App is used as a gateway and an Open stack cloud is used for the purpose of storing, computing, and analyzing the data. Moreover, Blynk APP uses to register the data into the system initially that helps in detecting the intruders. Blockchain technology helps to give privacy and preservation for the data with its unique features like transparency, immutability, and distributed nature[46]. Hence, in the proposed system, the instructions given to the IoT based vehicle and the vehicle responses are maintained in the blockchain as transactions.

Figure 1 shows the overview of the proposed system. This system consists of three modules that operate simultaneously such as the design and development of virtual circuit based IoT components as a first module. The second module is deploying the data on the cloud environment [45] and the third module is deploying the data on blockchain environment.

As part of the design and development of the first module, all IoT components (VMSS) such as Node MCU, Arduino, Motor Drivers, Wheels, and Camera are interconnected. These components are deployed using a python program. Initially, the user needs to give instructions to the vehicle through mobile devices regarding its movement like Left, Right, Straight, and Back. These instructions are processed over VMSS components. Later the surroundings are monitored with the help of the attached camera to the vehicle. Simultaneously, the captured data is compared with the registered data via BLYNK APP. If any intruder is detected, the data is stored in the cloud as well as in blockchain through the gateway i.e BLYNK APP and public chain blockchian architecture. Figure 2 shows the flow of transactions among the objects of the proposed system.

In the second module, the hash value of the received data from the vehicle will be computed using the SHA-1 algorithm. Later this hash value is compared with existing data hash value. If both the hash values are the same, then the

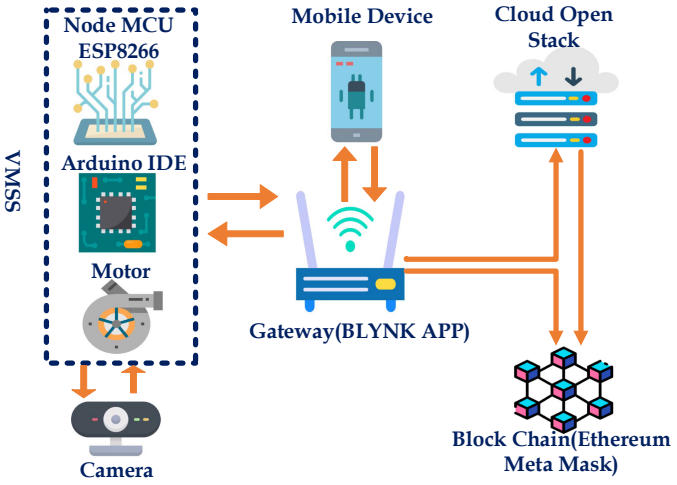

Fig. 1. Architecture of proposed methodology

Algorithm 1: Virtual circuit based IoT use case

```
Input: User's instructions as request (Left, Right, straight, Back)
Output: Vehicle movement & capture the data
User 'A' gives instructions to the vehicle through mobile devices
x ← Req[A]
Process the request based on deployed python program into Arduino connected
VMSS
Motor Driver [vehicle] ⟵ x
Capture the data by the camera
if intruder detects then
    y ← Data[Intruder]
else
    continue
end
```

received data is considered as belonging to the intruder, otherwise to the authorized person or vice-versa. This depends on which data has to be taken to do registration at the initial stage. This response is forwarded to the user through the VMSS monitor and the hash value is sent to the mobile device via a gateway.

The data is deployed on the public blockchain for improving privacy, efficiency, and computational costs. The instructions from the user to the vehicle and the responses from the vehicle are maintained on a blockchain as block transactions. Here, an Ethereum based public blockchain is used that requires smart contracts & wallet balance to maintain the data on the block as transactions. Before making a transaction, the wallet balance (eth) is verified. Here, a web-based Metamask Wallet is used to manage (eth) balance. For each transaction,

Algorithm 2: Deployment of the data on Cloud

Input: Data from VMSS i.e 'y'
Output: Intruder/authorized data as a response
Establish the connection with the VMSS through the gateway (BLYNK APP)
Computes and maintains hash values of the suspicious data instructed by the User in cipher text using a public key
H[i] ← Hash (*intruderdata*)
Analyze the received data
for $i = 1; i <= length\ [data]; i++$ **do**
    if *h [i]== Hash(y)* **then**
        Res ← Intruder otherwise Res ← authorized
    else
    end
end
Sends the response to VMSS monitor as well as hash value to mobile device

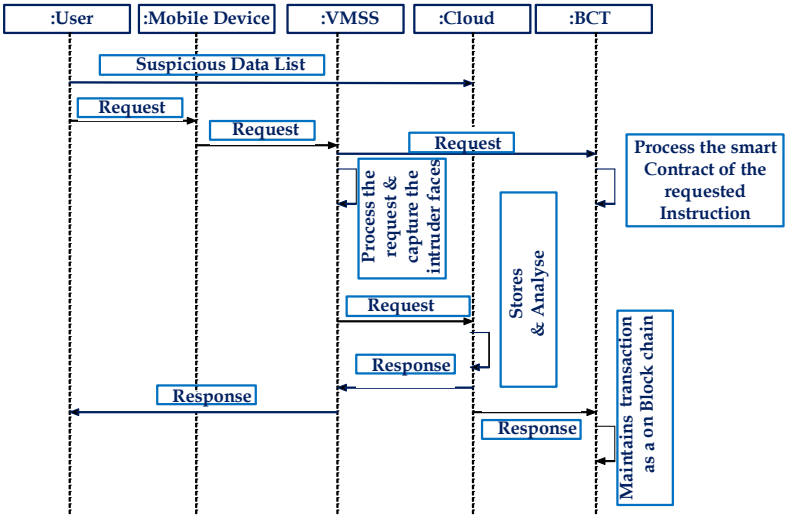

Fig. 2. Sequence of transactions in the proposed system

the wallet balance is reduced. After successful deployment, the transaction stores in a block. Later, this block joins into the blockchain. This block transaction is immutable, transparent, and distributed across all the connected nodes over this network.

Algorithm 3: Deployment of the data on Blockchain

```
Input : VMSS received Instructions from the users & vehicle Responses.
Output: Create immutable transactions over the blockchain and stores in a
  block
User 'A' gives instructions to the vehicle through mobile devices (VMSS)
x ← Req[A]
Deploy the smart contract over blockchain to maintains the instructions as
  transactions
if balance[wallet] >= Minimum then
    Block [i]=Txn
else
    exit
end
Response received from the cloud then repeat step 5
```

4 Conclusion and Future Work

Blockchain-based cloud-integrated IoT applications like intruder detection systems improve performance, security, and efficiency. The hybrid design in this work improves certain factors of the system such as data privacy and portability. These can be achieved by using one-way hashing algorithms. It extends security and privacy due to the immutable property of the blockchain. Another factor of this application is data transparency among the connected nodes over the network due to its distributed nature included in the architecture by default. The proposed system can be used to monitor and record illegal activities. In the future, we would like to implement the proposed system using UAV. To identify the intruders, we would like to consider and verify the faces of the intruders. To design and develop the blockchain, an Ethereum based Ganache blockchain along with a metamask wallet is planned.

References

1. Alazab, M., et al.: A hybrid wrapper-filter approach for malware detection. J. Netw. **9**(11), 2878–2891 (2014)
2. Alazab, M., Layton, R., Broadhurst, R., Bouhours, B.: Malicious spam emails developments and authorship attribution. In: 2013 Fourth Cybercrime and Trustworthy Computing Workshop, pp. 58–68. IEEE (2013)
3. Ali, M.S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., Rehmani, M.H.: Applications of blockchains in the Internet of Things: a comprehensive survey. IEEE Commun. Surv. Tutor. **21**(2), 1676–1717 (2018)
4. Anthi, E., Williams, L., Słowińska, M., Theodorakopoulos, G., Burnap, P.: A supervised intrusion detection system for smart home IoT devices. IEEE Internet Things J. **6**(5), 9042–9053 (2019)
5. Arshad, J., Azad, M.A., Amad, R., Salah, K., Alazab, M., Iqbal, R.: A review of performance, energy and privacy of intrusion detection systems for IoT. Electronics **9**(4), 629 (2020)

6. Baza, M., Lasla, N., Mahmoud, M., Srivastava, G., Abdallah, M.: B-ride: ride sharing with privacy-preservation, trust and fair payment atop public blockchain. IEEE Trans. Netw. Sci. Eng. (2019, in press)
7. Bhattacharya, S., Kaluri, R., Singh, S., Alazab, M., Tariq, U., et al.: A novel PCA-firefly based XGBoost classification model for intrusion detection in networks using GPU. Electronics **9**(2), 219 (2020)
8. Ch, R., Gadekallu, T.R., Abidi, M.H., Al-Ahmari, A.: Computational system to classify cyber crime offenses using machine learning. Sustainability **12**(10), 4087 (2020)
9. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., Faruki, P.: Network intrusion detection for IoT security based on learning techniques. IEEE Commun. Surv. Tutor. **21**(3), 2671–2701 (2019)
10. Chiramdasu, R.: Extended statistical analysis on multimedia concealed data detections. J. 161–165 (2019). http://iieta.org/journals/isi24(2)
11. Djenouri, D., Badache, N.: Struggling against selfishness and black hole attacks in MANETs. Wirel. Commun. Mob. Comput. **8**(6), 689–704 (2008)
12. Dwivedi, A.D., Malina, L., Dzurenda, P., Srivastava, G.: Optimized blockchain model for Internet of Things based healthcare applications. In: 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), pp. 135–139. IEEE (2019)
13. Dwivedi, A.D., Srivastava, G., Dhar, S., Singh, R.: A decentralized privacy-preserving healthcare blockchain for IoT. Sensors **19**(2), 326 (2019)
14. Ganapathy, S., et al.: A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications. Comput. Netw. **151**, 181–190 (2019)
15. Hakak, S., Khan, W.Z., Gilkar, G.A., Imran, M., Guizani, N.: Securing smart cities through blockchain technology: architecture, requirements, and challenges. IEEE Netw. **34**(1), 8–14 (2020)
16. Hu, M.S., Chen, L.H.: The application of embedded control and IoT technology in the automatic light-chasing vehicles. In: 2019 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE), pp. 362–365. IEEE (2019)
17. Irfan, S., Rupa, C., Vinay, K., Veni, M.K., Rachana, R.: Smart virtual circuit based secure vehicle operating system. In: 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 386–390. IEEE (2020)
18. Iwendi, C., et al.: Keysplitwatermark: zero watermarking algorithm for software protection against cyber-attacks. IEEE Access **8**, 72650–72660 (2020)
19. Jan, S.U., Ahmed, S., Shakhov, V., Koo, I.: Toward a lightweight intrusion detection system for the Internet of Things. IEEE Access **7**, 42450–42471 (2019)
20. Jindal, A., Aujla, G.S., Kumar, N.: Survivor: a blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment. Comput. Netw. **153**, 36–48 (2019)
21. Khalid, U., Asim, M., Baker, T., Hung, P.C., Tariq, M.A., Rafferty, L.: A decentralized lightweight blockchain-based authentication mechanism for IoT systems. Cluster Comput. 1–21 (2020)
22. Khezr, S., Moniruzzaman, M., Yassine, A., Benlamri, R.: Blockchain technology in healthcare: a comprehensive review and directions for future research. Appl. Sci. **9**(9), 1736 (2019)
23. Li, D., Deng, L., Lee, M., Wang, H.: IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning. Int. J. Inf. Manag. **49**, 533–545 (2019)

24. Li, X., Wang, Q., Lan, X., Chen, X., Zhang, N., Chen, D.: Enhancing cloud-based IoT security through trustworthy cloud service: an integration of security and reputation approach. IEEE Access **7**, 9368–9383 (2019)
25. Longstreet, P., Brooks, S.: Life satisfaction: a key to managing Internet & social media addiction. Technol. Soc. **50**, 73–77 (2017)
26. Ma, S., Deng, Y., He, D., Zhang, J., Xie, X.: An efficient NIZK scheme for privacy-preserving transactions over account-model blockchain. IEEE Trans. Dependable Secure Comput. (2020, in press)
27. Maddikunta, P.K.R., Gadekallu, T.R., Kaluri, R., Srivastava, G., Parizi, R.M., Khan, M.S.: Green communication in IoT networks using a hybrid optimization algorithm. Comput. Commun. **159**, 97–107 (2020)
28. Maddikunta, P.K.R., et al.: Unmanned aerial vehicles in smart agriculture: applications, requirements and challenges. arXiv preprint arXiv:2007.12874 (2020)
29. Maddikunta, P.K.R., Srivastava, G., Gadekallu, T.R., Deepa, N., Boopathy, P.: Predictive model for battery life in IoT networks. IET Intell. Transp. Syst. **14**(11), 1388–1395 (2020)
30. Markit, I.: The Internet of Things: a movement, not a market. Englewood, CO: IHS Markit (2017). Accessed 28 Dec 2018
31. Metlo, S., Memon, M.G., Shaikh, F.K., Teevno, M.A., Talpur, A.: Crowdsource based vehicle tracking system. Wirel. Pers. Commun. **106**(4), 2387–2405 (2019)
32. Mollah, M.B., et al.: Blockchain for future smart grid: a comprehensive survey. IEEE Internet Things J. (2020)
33. Niu, Y., Li, Y., Jin, D., Su, L., Vasilakos, A.V.: A survey of millimeter wave communications (mmWave) for 5g: opportunities and challenges. Wirel. Netw. **21**(8), 2657–2676 (2015)
34. Nobakht, M., Sivaraman, V., Boreli, R.: A host-based intrusion detection and mitigation framework for smart home IoT using openflow. In: 2016 11th International conference on availability, reliability and security (ARES), pp. 147–156. IEEE (2016)
35. Priya, K.L.S., Rupa, C.: Block chain technology based electoral franchise. In: 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 1–5. IEEE (2020)
36. Qiang, W.: Performance and security in cloud computing. J. Supercomput. **75**(1), 1–3 (2018). https://doi.org/10.1007/s11227-018-2671-4
37. Rasool, S., et al.: Blockchain-enabled reliable osmotic computing for cloud of things: applications and challenges. IEEE Internet Things Mag. (2020)
38. Reddy, G.T., Sudheer, K., Rajesh, K., Lakshmanna, K.: Employing data mining on highly secured private clouds for implementing a security-ASA-service framework. J. Theor. Appl. Inf. Technol. **59**(2), 317–326 (2014)
39. RM, S.P., et al.: Load balancing of energy cloud using wind driven and firefly algorithms in internet of everything. J. Parallel Distrib. Comput. **142**, 16–26 (2020)
40. RM, S.P., et al.: An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IOMT architecture. Comput. Commun. **160**, 139–149 (2020)
41. Rupa, C.: An integrated digital authentication mechanism for intrusion detection system. In: Big Data Analytics for Smart and Connected Cities, pp. 158–169. IGI Global (2019)
42. Sabir, N., Memon, A.A., Shaikh, F.K.: Threshold based efficient road monitoring system using crowdsourcing approach. Wirel. Pers. Commun. **106**(4), 2407–2425 (2019)
43. Salah, K., Rehman, M.H.U., Nizamuddin, N., Al-Fuqaha, A.: Blockchain for AI: review and open research challenges. IEEE Access **7**, 10127–10149 (2019)

44. Sharma, P.K., Kumar, N., Park, J.H.: Blockchain-based distributed framework for automotive industry in a smart city. IEEE Trans. Indu. Inform. **15**(7), 4197–4205 (2018)
45. Singh, S., Jeong, Y.S., Park, J.H.: A survey on cloud computing security: issues, threats, and solutions. J. Netw. Comput. Appl. **75**, 200–222 (2016)
46. Singh, S., Ra, I., Meng, W., Kaur, M., Cho, G.: SH-BlockCC: a secure and efficient Internet of Things smart home architecture based on cloud computing and blockchain technology. Int. J. Distrib. Sens. Netw. **15**(4), 1–18 (2019)
47. Truong, N.B., Sun, K., Lee, G.M., Guo, Y.: GDPR-compliant personal data management: a blockchain-based solution. arXiv preprint arXiv:1904.03038 (2019)
48. Wang, H., Qin, H., Zhao, M., Wei, X., Shen, H., Susilo, W.: Blockchain-based fair payment smart contract for public cloud storage auditing. Inf. Sci. **519**, 348–362 (2020)
49. Xiao, Y., Zhang, N., Lou, W., Hou, Y.T.: A survey of distributed consensus protocols for blockchain networks. IEEE Commun. Surv. Tutor. (2020, in press)